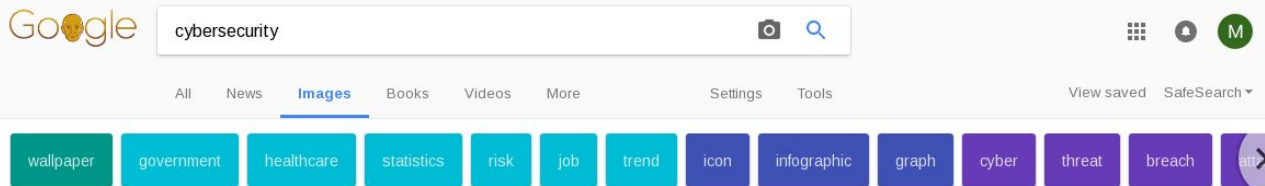# NSLS-II Controls/IT

Cybersecurity

- Is that NSLS-II !?
- Other Synchrotrons ?! (could be Apple HQ)

- With high user turnover and users from all over, synchrotrons are interesting indirect targets!

Other takeaways:

- Beware of people in hoodies, ascii text, numbers and schematics.

- Oh wait, they're friendly!

- Considering deploying "cybersecurity" keys on all keyboards during May 2018 shutdown.

- Apparently Cyan is the new Green?

Cybersecurity tasks

- It's an integral part of almost everything the IT group does

- Downside is, when people mention "cybersecurity work" they usually mean paperwork and related tasks required by BNL/DOE (eg. NIST.SP.800-53)

  - NSLS-II IT System Security Plan (for accelerator) (accepted, with 14 POAMs)
  - NSLS-II Beamline Security Plan (WIP)

but

  - BNL Cyber is working hard to minimize the amount of documentation required for each facility/subsystem

but

  - Still a ways to go. Could be a fulltime position; available resources are much less.
  - As things are, we struggle to meet deadlines for commitments to DOE

Real Security Talk® : a choose your own adventure presentation

What do you want to know about:

- DOE paperwork?

- Implementation details?

Real Security Talk®

How do we secure all this stuff? Especially the stuff with no builtin security and/or known issues?

- Isolation
- compartmentalization

questions?

POAMs

Plan of Action and Milestones (POA&M or POAM)

- mandated by Federal Information Systems Management Act (FISMA)
- tracked by BNL DOE Site Office (BHSO) and higher within DOE

- formally track findings from reviews and audits to completion

https://www.dhs.gov/sites/default/files/publications/4300A-Handbook-Attachment-H-POAM-Guide.pdf